SECURITY AND HOSTING

Mortgage Computer
Ogden, Utah

Preface

The Hosted Server uses industry standard 128-bit data encryption with SSL public key/private key (PKI) certificates. **All** information relayed between your workstation and the server is encrypted with this method.

Each company hosted by Mortgage Computer will have the option to include an ACL (access control list) limiting the IP addresses by user name that are allowed to connect to the MC Software. With this option controlled by your administrator you can allow some users to work remotely while limiting others to work from the office only.

The ColdFusion Server and the SQL Data Base server are dedicated, separate servers allowing Mortgage Computer to limit direct access to the ColdFusion server only. This allows ColdFusion to control all access to and from the SQL Data Base via program control rather than direct Data Base access by each authenticated user.

The network is among the best-connected hosting facilities in the world. The data centers are implemented through a high-speed network specifically designed for dedicated server hosting. We have invested in both network equipment and backbone connections to ensure that customers get the fastest access possible to their content and applications.

The network facilities have multiple network connections to different Internet backbones, allowing data to be distributed though many sources – meaning that the facility is not dependent upon any single Internet backbone.

MC Software includes two levels of user name/password authentication. The first is set up and controlled by Mortgage Computer and assigned one per company. The second is assigned by your internal administrator, allowing you to regulate access to specific areas in MC Software by user name. Both levels follow established password criteria, including eight-character minimum, required combinations of alphabetic and numeric characters (minimum three of each). Password aging requiring users to change their passwords every 30 days and does not allow re-use of the current password.

Property of Mortgage Computer.
This material may not be copied or duplicated without permission from Mortgage Computer.
This material cannot be shown or distributed to anyone not licensed by Mortgage Computer.
Failure to comply will result in prosecution to the fullest extent of the law.

Security and Hosting

Contents *- Updated October 18, 2013*

System Requirements 4

The Data Center 5
- The Facilities 6
- Securing The Planet 8

Required Internet Explorer Browser Settings for MC Software 23

MC Software 31
- MC Software Company Login 33
- MC Software Web Login 34
- Update Password 35
- MC Software Helpful Hints 36
- MC Software Security 38

System Requirements

Supported Systems

Windows 7 or Windows 8 with all current service packs and critical updates applied. MC suggests at least 4 gig minimum system memory. Also make sure your CPU, video, network card, etc., meet Microsoft's requirements for the version of Windows you are running.

1. High speed Internet connection (at least DSL speed, cable, T1, or higher recommended).

2. Adobe Reader 10 or higher, 11 is recommended (free download from adobe.com). All reports are created in PDF format. Adobe Acrobat is required if you would like to create Loan Processing application and/or closing documents in PDF format. Loan Processing reports are already created in PDF format.

3. Adobe Flash Player 10 or higher, 11 is recommended (free download from adobe.com). Functions within MC Software and WebApp require Flash Player.

4. Windows graphical printer(s) set up as local or network printer(s) to the workstation(s) being used. For document printing, it is recommended to be a laser printer that allows letter- and legal-sized paper to be available at the same time as most document packets contain both paper sizes.

5. Local workstation Administrator login required at the workstation for initial installation of the Loan Processing forms viewer application.

6. Internet Explorer 9 or 10 with all critical updates. MC Software sites added as trusted sites with default level on those sites set to low. The specific list will be given during installation. Additional specific settings given at the time the trusted site list is given as well.

7. All toolbar/toolbar add-ons in Internet Explorer **must** be removed as they have their own security settings and pop-up blocker settings separate from the Internet Explorer settings and may interfere with the specific settings in Internet Explorer for MC Software.

8. Make sure you do not have Microsoft Network Security Policies in place that will interfere with the Internet Explorer settings for MC Software along with not blocking installation of Active X controls for the Forms Viewer.

   Please note: This means a workstation, not ***thin client***. The Wolters Kluwer Document Viewer requires Active X controls to be installed on the local workstation and this will not work via most thin client.

The Data Center

Data Center, Dallas, Texas

The Facilities

The data center that houses the servers is located in Dallas, Texas. The facility offers complete redundancy in power, HVAC, fire suppression, network connectivity, and security. With over 35,000 square feet of raised floor and 15,000 square feet of static-free tile, it has an offering to fit any need. The facility sits atop multiple power grids driven by TXU electric, and has multiple Liebert and PowerWare UPS battery backup power and onsite permanent generator power. The HVAC systems are a combination of glycol, chilled water, and condenser units by Liebert and Data Aire to provide redundancy in cooling coupled with six managed backbone providers. Twelve more third-party backbone providers are available in the building via cross-connect. Fire suppression includes a pre-action dry pipe system in both facilities including VESDA (very early smoke detection apparatus) along with over 600 smoke detectors. Security is also a concern for customers, so all facilities are key card access with CCTV for maximum security. All visitors to the data centers must check in and out of the facility. The goal is to provide maximum redundancy in every facet of the data center environment to facilitate 100% uptime for your entire hosting infrastructure.

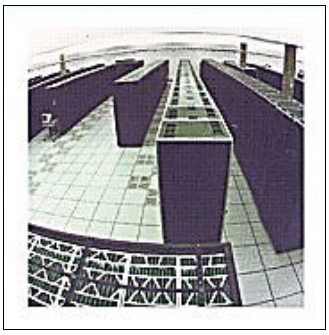
CFDynamics

Monitoring

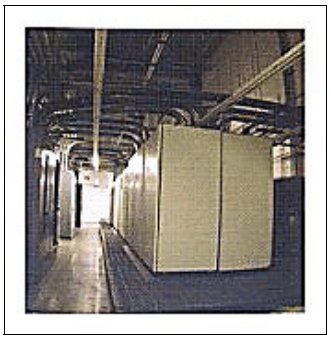
CFDynamics.com provides 24x7 monitoring on customer and infrastructure equipment to ensure maximum availability.

Network Infrastructure

The internal network architecture utilizes the Enterprise routing and switching engines from Juniper and Cisco. We utilize Juniper M20 routers as border routers, Cisco 6500 series switches in the distribution layer, Cisco 6500 and 5500 switches in the aggregation layers, and Cisco 3500 and 2900 series switches at the customer layer. The network is fully meshed and redundant with six backbone providers. The current network consists of, UUNet (GigE), Level 3 (GigE), Time Warner (GigE), Global Crossing (GigE), Verio (GigE), and ATT (DS3).



Inside the computer room

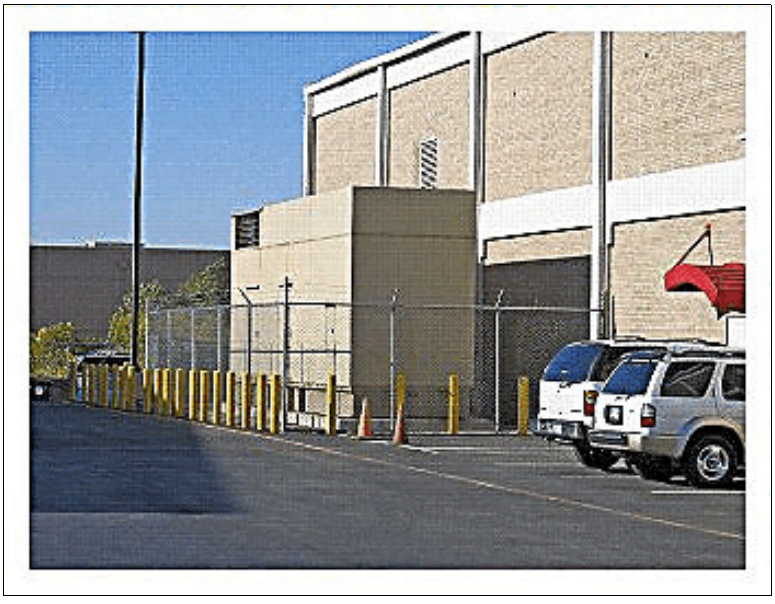


Power equipment room

Security monitoring room

Security monitored 24x7

Diesel generators outside data center



One of the two diesel generators

Securing The Planet

The Internet has experienced a surge in malicious traffic including denial of service attacks, worms and viruses. Worldwide, in the past year, 64 percent of businesses have experienced a worm or virus attack – an increase of 45 percent as compared to 2003 – and 19 percent have been hit by denial of service attacks according to the Global Information Security Survey. The global financial impact of viruses alone was $12.5 billion in 2003 and the increase in these incidents shows a growing sophistication on the part of those that launch the attacks, according U.S. research firm Computer Economics as reported in Computing Magazine.

> *The question is not "if" you should look at security services, but "have you already deployed security measures, and are you staying on top of new security threats and developments?"* Craig Rodenberg, VP, Information Security – The Planet

The Planet has created strategic partnerships with a select group of vendors to intensate its already state-of-the-art security system. A depth-of-defense strategy has been employed to deepen the layers of network protection and a Security Operations Center (SOC) created, staffed with CISSP and GIAC certified security engineers, with the goal of making our networks and client networks impervious to intrusion and attack.

Between ~14 Gbps and ~8 Gbps of traffic enters The Planet at any given moment. That traffic originates from 16 different carriers through Equinix, referred to internally as location D3, located at the Infomart. All traffic from Equinix, with the exception of unmetered, unfiltered MatriXtreme traffic, passes through multiple, dense layers of network security. In addition to the security provided at the network level, The Planet offers a multitude of security services that clients may also choose to utilize.

The Planet's layers include:

- Attack Prevention Services
- Detection and Incident Response Services
- Threat Elimination Services

Attack Prevention Services

Attack Prevention Services analyze attack readiness and provide recommendations for remediation. Prevention services are available with every server hosted at The Planet and include:

- Ozone Access Control List Management
- Virtual Private Network Tunnels
- Vulnerability Assessments
- Penetration Testing
- Operating System Hardening
- Custom Cryptographic Services

Ozone Access Control List Management

Web servers must be accessible, which makes them vulnerable to attack. Firewalls can be used to limit exposure to these servers, but they can still be overtaken by traffic directed at TCP and UDP ports allowed through the firewalls. Networks and hosts are substantially more secure with access control lists (ACLs) in place.

An ACL is a set of controls that filters out unwanted traffic and provides a logical, intuitive mechanism for defining security policies. The Planet's Ozone implements ACLs on virtual local area networks (VLANs) protecting servers from exploits on unused TCP and UDP ports.

Ozone offers five environments for VLAN ACL protection:

- A Windows server environment (Windows 2000 and 2003)
- A Unix server environment (Redhat, FreeBDS, Debian)
- An OS neutral server environment (Windows 2000, Windows 2003, Redhat, FreeBDS, Debian)
- A Game server environment (any OS) using templates designed by The Planet's security experts
- An Explicit Generic Deny Environment (any OS) that blocks well known vulnerable ports

A number of rule-based packet filters are available from which to choose within each environment – one filter per VLAN is allowed. These filters are not designed to take the place of a true firewall, and do not offer the same type of functionality of performance.

With Ozone:

- The Planet is providing a high-end security system to their clients that would be prohibitively expensive to purchase and maintain on their own.
- The Planet Security Engineers are available to constantly review current threats on the Internet and add or remove ports in danger
- Filters can be added or removed by the customer once an hour using The Planet's proprietary Web portal, ORBIT℠.

Ozone is aggressively priced at $20 per VLAN (one template is allowed per VLAN). *An additional fee is charged for moving servers between VLANS.* Customers may add VLAN filtering to an existing VLAN or order a filter template upon signup.

Virtual Private Network Tunnels

In the new world of networking, businesses can rely on VPN technology to utilize the Internet as their secure networking backbone. A VPN offers significant savings on communications costs while allowing businesses to tap into a reliable network. VPNs can connect multiple offices, remote users, business partners, and clients through the Internet. VPN solutions include hardware, software, firewall-to-firewall, router-to-router, concentrators, remote access, LAN-to-LAN, and extranets.

Even the most seasoned veteran needs networking assistance from time to time. The Planet's Cisco Certified Administrators are available to develop a VPN solution whether for businesses exchanging confidential data, creating multi-site access to corporate servers and databases, or simply protecting communications between vendors and employees.

Our Security Engineers are available to assist with routers, firewalls, load balancers, backend networks, network configurations, VLANs, subnetting, static routing and network traffic monitoring; to design a new network or revamp a current one.

Our network administrators are available to design a new network or revamp a current one, to assist with routers, firewalls, load balancers, backend networks, network configurations, VLANs, subnetting, static routing and network traffic monitoring. Virtual Private Network Tunnel assistance is available at an additional cost per hour or per project.

Vulnerability Assessments

Vulnerability assessments identify systems and components operating on servers, and test them using a vulnerability database that is updated by The Planet on a daily basis. The assessment generates a list of known vulnerabilities delivered to The Planet customer. The customer can either repair these vulnerabilities on their own, or have The Planet technicians apply the appropriate patches and updates. "Light" Vulnerability Assessments are provided at no additional cost, Full Vulnerability Assessments are available with Managed Security Services).

Penetration Testing

The Planet's CISSP and GIAC certified security engineers, using industry-standard and underground tools and techniques, will perform a full-fledged attack of a hosted server to determine just how safe that server is against malicious penetration. Penetration test results tell the client which of their systems is the most vulnerable to allow them to concentrate on upgrading and updating those weaknesses. Penetration testing and vulnerability assessments complement one another, and are often required for industry compliance with standards such as Visa certification, FDIC certification, HIPAA compliance, GLB act compliance and others. Penetration Testing is a service available to all customers.

Operating System Hardening

OS Hardening, a process of securing, a server can serve to mitigate the risk of being hacked or of suffering a denial of service attack by over 90 percent. Hardening techniques hide the fingerprints that hackers use to identify what is running on a system or sends them misleading information that identifies the type system being run. Operating System hardening causes hacks to be completely ineffective. Hardening tactics are frequently updated, and require high levels of security and system administration expertise. They are most effectively administered by The Planet's security engineers at the time a server is provisioned.

Custom Cryptographic Services

Upon request, The Planet's Security Engineering team can provide a custom cryptographic schema for our customer's data. This can be whole-drive encryption or individually encrypted directories. This additional measure of protection provides audit compliance, cutting-edge security of valuable E-commerce data and secure storage of Privacy Act data. Cryptographic services are provided after a thorough consultation with the customer. Standard algorithms are available in 128, 256 and 448 bit key lengths.

Detection and Incident Response Services

Detection and Response Services recognize and stop attempted intrusions, prevent further intrusions from occurring, and provide a real-time alert to The Planet's Security Operations Center. These services are continuously monitored by security engineers and include:

- Arbor Peakflow DDoS Detection
- Firewall Protection administered by our engineers, experts in Cisco Pix, Watchguard, Checkpoint and Cyberguard
- TippingPoint's Unity One 2400 in-line network intrusion detection and prevention system
- Cisco Guard DDoS Mitigation deployed at the network edge in the event of an event detected by Arbor
- ISS RealSecure Host Based Intrusion Detection System
- SecurePack Security Reporting
- Server Event Monitoring Services
- Server "Delta" Hardening
- System Integrity Checking

Arbor Peakflow DDoS Detection

A Flood or DDoS attack is a planned event whereby an individual instructs an army of "zombies"– computers that have been put under the control of a malicious hacker via the use of scripts, sometimes without the knowledge of the computer owner – to send a flood of requests to a server. The goal of the attack is to shut out legitimate requests and compromise the availability of the server. Although targeted to a particular server or site, a DDoS attack may impact the availability of 200-300 additional machines in a packet switching network. Flood attacks can be generated from 'real' IP hosts or may be spoofed to hide the real identify of the attackers.

The number of attacks has increased and become increasingly more complex as sophisticated hackers continue to create new attack schemes and make the scripts widely available on the Internet. There are three types of denial-of-service attacks:

- Volume flood attacks are designed to generate huge volumes of traffic, saturate the network infrastructure and 'fill-up the pipe' so legitimate traffic cannot get through to the destination host.
- Resource exhaustion attacks are often complex flood attacks designed to mimic real client activity and exhaust a server's resources. Usually, these attacks generate less traffic than a volume flood, but not always, and are trickier to block.
- Other complex denial-of-service attacks are delivered by specially crafted packets usually to exploit some vulnerability on the server and kill the service. Network or host-based IPS must be used for this type of attack.

The Planet monitors all traffic entering the network, except MatriXtreme, for possible network floods or Distributed Denial of Service (DDoS) with Arbor Peakflow DDoS Detection. Arbor Peakflow, a standard service available at no additional cost to the client, is used in conjunction with Cisco® Guard XT 5650 DDoS Mitigation Appliance and the TippingPoint IPS system.

Arbor collects information from Internet routers and develops a baseline and color graph of normal traffic. An abnormal volume of traffic, or other deviation from normal, generates an event record. The graph depicting traffic patterns is used by NOC/SOC to confirm the attack and DDoS mitigation is begun.

Firewall Protection

Our firewall administration option allows our administrators, experts in Cisco Pix, Watchguard, and Checkpoint and Cyberguard firewall appliances, to manage a customer's firewall over a secure console connection within the datacenter. Our security experts keep the firewall up to date, make routine or emergency changes, or assist in developing security policies.

We currently offer the following firewall protection from Cyberguard and Cisco:

- Cyberguard SG 630 (PCI)
- Cyberguard SG 550
- Cyberguard SG 575
- Cisco PIX 501 – UR
- Cisco PIX 506E
- Cisco PIX 515E-R
- Cisco PIX 515E-UR
- Cisco PIX 525-R
- Cisco PIX 525-UR
- Cisco PIX 535-R
- Cisco PIX 535-UR

The **Cyberguard SG 630** is a cost-effective firewall/VPN solution packaged on a PCI card. By offloading all firewall and VPN processing from the host computer, the SG630 ensures high performance and throughput with the convenience of remote management and simplified installation. Unlike "co-processing" products, the SG630 is an advanced, self-contained multitasking stateful firewall and VPN appliance. It includes a RISC processor, encryption accelerator for IPsec VPN traffic and two Ethernet interfaces for host and LAN communications. The SG630 packs the power of an SG firewall/VPN solution while eliminating the cabling, space and power requirements of an external firewall appliance.

The **Cyberguard SG 550** Security Appliance is a feature-rich, compact, network security device, that is well suited to protecting small branch offices of medium sized enterprises. The SG550 enables remote office networks to easily connect their PCs and servers to the Internet via broadband (ADSL, cable, SHDSL, T-1 and T-2 circuits, etc.) or narrow-band (modem or ISDN). Should the broadband connection fail the SG550 can fail over to the narrow band backup connection, ensuring uptime. A powerful stateful-inspection firewall, service-based intrusion detection blocking and advanced Internet connection sharing protect the branch office network from the Internet.

The **Cyberguard SG575** Security Appliance enables administrators to deploy a powerful, fully integrated firewall, VPN and Intrusion Detection System (IDS) solution at a fraction of the cost of a standalone IDS. The SNORT-based IDS adds an extra security layer by detecting attacks and alerting administrator so that countermeasures can be implemented quickly before the network is compromised. The SG575 provides central site VPN, firewall and session load balancing capabilities with the capacity to securely connect hundreds of mobile and remote employees. It improves business efficiencies by increasing Internet and VPN performance, maximizing uptime, and ensuring rock solid security.

The **Cisco PIX® 501** Security Appliance delivers enterprise-class security for small offices and teleworkers in a reliable, plug-and-play purpose-built appliance. Ideal for securing high-speed "always on" broadband environments, the Cisco PIX 501 Security Appliance, which is part of the world-leading Cisco PIX Security Appliance Series, provides robust integrated security capabilities, small office networking features, and powerful remote management capabilities in a compact, all-in-one solution. The PIX 501 includes an integrated 4-port Fast Ethernet (10/100) switch and a Fast Ethernet (10/100) interface. Ideal for securing high-speed broadband environments, the Cisco PIX 501 delivers up to 60 Mbps of firewall throughput, 3 Mbps of Triple Data Encryption Standard (3DES) VPN throughput, and 4.5 Mbps of Advanced Encryption Standard-128 (AES) VPN throughput.

The **Cisco PIX® 506E** Security Appliance delivers enterprise-class security for remote office/branch office environments in a robust, purpose-built appliance. Ideal for securing Internet connections for remote/branch offices, the Cisco PIX 506E Security Appliance, which is part of the world-leading Cisco PIX Security Appliance Series, provides a wide range of rich integrated security capabilities and powerful remote management capabilities in a cost-effective, high performance solution. The PIX 506E delivers a multilayered defense for remote offices through rich security services including stateful inspection firewalling, protocol and application inspection, virtual private networking (VPN), in-line intrusion protection, and rich multimedia and voice security in a single device. The state-of-the-art Cisco Adaptive Security Algorithm (ASA) provides rich stateful inspection firewall services, tracking the state of all authorized network communications and preventing unauthorized network access.

The **Cisco® PIX® 515E** Security Appliance delivers enterprise-class security for small-to-medium business and enterprise networks, in a modular, purpose-built appliance. Its versatile one-rack unit (1RU) design supports up to six 10/100 Fast Ethernet interfaces, making it an excellent choice for businesses requiring a cost-effective, resilient security solution with DMZ support. Part of the market-leading Cisco PIX Security Appliance Series, the Cisco PIX 515E Security Appliance provides a wide range of rich integrated security services, hardware VPN acceleration, and powerful remote management capabilities in an easy-to-deploy, high-performance solution.

The Cisco PIX 515E "Restricted" **(PIX 515E-R**), restricted software license model, provides an excellent value for organizations looking for robust Cisco PIX Security Appliance services with minimal interface density and modest VPN throughput requirements. It includes 32 MB of RAM, two 10/100 Fast Ethernet interfaces, and support for one additional 10/100 Fast Ethernet interface.

The PIX 515E "Unrestricted" (**PIX 515E-UR**), unrestricted software license model, extends the capabilities of the family with support for stateful failover, additional LAN interfaces, and increased VPN throughput via integrated hardware-based VPN acceleration. It includes an integrated VAC or VAC+ hardware VPN accelerator, 64 MB of RAM, two 10/100 Fast Ethernet interfaces, and support for up to four additional 10/100 Fast Ethernet interfaces. The Cisco PIX 515E-UR also adds the ability to share state information with a hot-standby Cisco PIX Security Appliance for resilient network protection.

The **Cisco® PIX® 525** Security Appliance delivers enterprise-class security for medium-to-large enterprise networks, in a reliable, purpose-built appliance. Its modular two-rack unit (2RU) design incorporates two 10/100 Fast Ethernet interfaces and supports a combination of up to six additional 10/100 Fast Ethernet interfaces or three additional Gigabit Ethernet interfaces, making it an ideal choice for businesses requiring a high performance, Gigabit Ethernet-ready solution that provides solid investment protection. Part of the market-leading Cisco PIX Security Appliance Series, the Cisco PIX 525 Security Appliance provides a wide range of rich, integrated security services, hardware VPN acceleration, and powerful remote management capabilities in a cost-effective, highly-resilient solution.

The Cisco PIX 525 Restricted (**PIX 525-R**), restricted software license model, provides an excellent value for organizations looking for robust Cisco PIX Security Appliance services with Gigabit Ethernet support, medium interface density and moderate VPN throughput requirements. It includes 128 MB of RAM, two 10/100 Fast Ethernet interfaces, and support for up to four additional 10/100 Fast Ethernet or three Gigabit Ethernet interfaces.

The Cisco PIX 525 Unrestricted (**PIX 525-UR**), unrestricted software license model, extends the capabilities of the security appliance with support for stateful failover, additional LAN interfaces, and increased VPN throughput via integrated hardware-based VPN acceleration. It includes an integrated VAC or VAC+ hardware VPN accelerator, 256 MB of RAM, two 10/100 Fast Ethernet interfaces, and support for up to six additional 10/100 Fast Ethernet or three Gigabit Ethernet interfaces. The Cisco PIX 525-UR also adds the ability to share state information with a hot-standby Cisco PIX Security Appliance for resilient network protection.

The **Cisco® PIX® 535 Security Appliance** delivers enterprise-class security for large enterprise and service provider networks, in a high performance, purpose-built appliance. Its highly modular three-rack unit (3RU) design supports a combination of up to 10 10/100 Fast Ethernet interfaces or nine Gigabit Ethernet interfaces as well as redundant power supplies, making it an ideal choice for businesses requiring the highest levels of performance, port density, reliability, and investment protection. Part of the market-leading Cisco PIX Security Appliance Series, the Cisco PIX 535 Security Appliance provides a wide range of rich, integrated security services, hardware VPN acceleration, and powerful remote management capabilities in a highly scalable, high-performance solution.

The Cisco PIX 535 Restricted (**PIX 535-R**), restricted software license model, provides an excellent value for organizations looking for robust Cisco PIX Security Appliance services with gigabit firewall throughput, high interface density, maximum investment protection, and moderate VPN throughput requirements. It includes 512 MB of RAM, two 10/100 Fast Ethernet interfaces, and support for up to six additional 10/100 Fast Ethernet or eight Gigabit Ethernet interfaces.

The Cisco PIX 535 Unrestricted (**PIX 535-UR**), unrestricted software license model, extends the capabilities of the security appliance with support for stateful failover, additional LAN interfaces, and increased VPN throughput via integrated hardware-based VPN acceleration. It includes an integrated VAC or VAC+ hardware VPN accelerator, 1 GB of RAM, two 10/100 Fast Ethernet interfaces, and support for up to eight additional 10/100 Fast Ethernet or nine Gigabit Ethernet interfaces. The Cisco PIX 535-UR also adds the ability to share state information with a hot-standby Cisco PIX Security Appliance for resilient network protection.

TippingPoint's Unity One

The Planet has upgraded its existing intrusion detection system to TippingPoint's Unity One 2400 Intrusion Prevention System (IPS). TippingPoint is a robust, high-performance IPS that is highly scalable – can easily grow with The Planet – and is able to filter a very high volume of traffic with virtually no network latency – no network delay – while performing thousands of simultaneous checks on each packet flow.

TippingPoint was the only participant granted the prestigious NSS Gold Award by the NSS Group, the world's foremost network and security testing organization, in their first comprehensive security and performance tests for IPS systems in January 2004.

TippingPoint is deployed between the Internet routers and each Data Center to provide deep packet filtering of all network traffic entering or leaving The Planet (except MatriXtreme) to remove malicious, unwanted traffic before it is routed to customer networks. TippingPoint's Digital Vaccine Service combines signature-based detection of known attacks – from a library of thousands of known signatures – with complex filtering mechanisms that detect protocol, application and statistical anomalies. The Vaccine delivers new filters on a weekly, or sometimes daily, basis to maintain protection for the latest vulnerabilities, exploits, viruses and rogue applications. TippingPoint prevents the identified malicious traffic from entering the network and being passed on to the client's server.

With TippingPoint, The Planet is delivering:

- A high-end security system that might be prohibitively expensive to purchase independently.
- Highly trained Planet engineers to stay on top of intelligence reports and announcements of threats to data security, and to quickly test and implement needed patches and upgrades.
- A Security Operations Center (SOC) that proactively monitors for security threats and escalates potential security problems to an experienced team of GIAC and CISSP certified security engineers. Working together, the SOC and Security Engineering teams provide real-time security incident response services and notify clients before attacks result in server compromise or downtime.

The TippingPoint reporting service is being integrated into The Planet's Orbit™ customer portal.

Cisco Guard DDoS Mitigation

The Planet handles a DDoS attack with Cisco® Guard XT 5650 DDoS Mitigation Appliance. When a flood attack is detected by Arbor, the SOC uses the traffic graphs to confirm the attack and enable Cisco® Guard. The Guard diverts the flood of traffic away from its intended path and into one of a configuration of Guard farms placed at Equinix near the very edge of the network.

The Guard system then filters the traffic using multiple interactive layers of defense that recognize and block many types of flood attacks. Filtering and active verification technologies enable rapid protection against many types of assaults, even ones that have never been seen before. Rate-based filtering, advanced anomaly recognition, source verification, and anti-spoofing technologies are used to identify and block individual attack flows.

Protocol analysis and rate limiting features help ensure that only valid traffic gets through in volumes that won't compromise a server. The Guard system does not interfere with regular production traffic. It keeps sites operational even during massive flood attacks that would otherwise disrupt or completely disable the site, and maintains a flow of legitimate traffic with no obvious degradation of services to legitimate users.

The Guard reporting service has been integrated into The Planet's Orbit™ customer portal letting customers under flood attack review hourly reports and graphs of activity and protection being provided by The Planet. All traffic entering The Planet network, except MatriXtreme, is monitored for DDoS attacks and benefits from DDoS mitigation at no additional cost to the client.

ISS RealSecure Host Based Intrusion Detection

The Planet now partners with Internet Security Systems (ISS), a premier security research, products and Services Company, for host-level protection. ISS has served the Global 500, as well as world governments, for the last decade. ISS RealSecure employs signature-based detection, sophisticated protocol analysis, and behavioral pattern analysis to block both known and unknown attacks. Signatures & analysis updates are provided by the highly regarded ISS X-Force research team.

RealSecure complements the network protection by safeguarding the underlying operating system from operating system exploits and application vulnerabilities. ISS Real Secure:

- Uses automated defensive actions to deny server attacks.
- Is monitored 24x7 in The Planet's SOC.
- Provides the server with end-to-end protection including file integrity monitoring.

All ISS Real Secure alarms are responded to by The Planet's experienced team of GIAC and CISSP certified security engineers. RealSecure, available for both Linux and Windows, is Windows Server 2003 and Windows 2000 Server Certified, is a fully-managed service available to all customers as a standard service feature on Total Control and Focus Series servers, and for $10 per month on Service Matrix servers.

SecurePack Security Reporting

The Planet's all new security services reporting is available through SecurePack. Customers receive access to Arbor, TippingPoint, Cisco Guard XT network and ISS host-based reporting, as well as firewall graphs. SecurePack is the most comprehensive security service available in the hosting marketplace. It will be a standard feature of the soon-to-be-launched FOCUS Series server line.

Server Event Monitoring Services

The Planet can provide highly granular monitoring of security specific events which are recorded by Syslog or Windows Event Log. Alert criteria can be set for events such as failed user passwords, password grinding, abnormal service or daemon behavior, service or daemon abuse, application brute forcing attempts or attempted privilege escalation. These additional measures can detect highly discrete attempts to compromise server integrity, and engage our Security Engineering team to respond.

Server "Delta" Hardening

The Planet's Security Engineering team can perform regularly scheduled Vulnerability Assessments to assist customers in tracking security problems induced by applications code changes, server updates, software additions and configuration changes. The Planet's Security Engineering team will alert the customer to detected security problems, and propose changes which will resolve the problem giving the customer the advantage of a continuously hardened server.

System Integrity Checking

System Integrity checking uses a database which monitors important files on the system and their file attributions, such as permissions, user, group, and number of links. Also, an encrypted checksum of each file is created. Tracking this information allows The Planet to set alarm criteria for unauthorized server changes and malicious user activity.

Threat Elimination

When new vulnerabilities are detected against any managed system, The Planet has a variety of responses available:

- Managed Operating System Update Services
- Server Administrative Services
- Incident Response by CISSP Certified Security Professionals
- Application Specific Updates

Managed Operating System Update Services

The Planet provides comprehensive Microsoft, Sun Solaris, and Red Hat Linux update and security patch services. RedHat Linux customers are subscribed to the Red Hat network at the Enterprise level. Microsoft customers are configured with Windows Update, which is monitored and managed centrally by the Information Security team. General release patches are applied using a maintenance window defined by the customer using Orbit. Security updates are typically tested and installed within eight to 20 hours of their release from Microsoft, Sun and Red Hat. The Planet's security engineers also monitor Cert and SANS advisories, Sun Solaris Patch Club, Slashdot, Microsoft TechNet and other operating system watchdog services to stay on top of the latest security issues and alerts. This additional assistance may be available at no extra charge, depending upon the Managed Service Level of the servers to be administrated.

Server Administrative Services

The Planet's Network Operations Engineers are available to assistance with server administration tasks that provide additional protection. These tasks might include adjustment to the operating system in order to match new service requirements, installing software, and maintaining user policies. This additional assistance may be available at no extra charge, depending upon the Managed Service Level of the servers to be administrated.

Incident Response by Certified Security Engineers

The Planet's Security Engineering Team is staffed by CISSP and GIAC certified security engineers. The Security Engineering Team is available 24/7/365 to resolve automated security services and proactively keep The Planet's network, and all servers in that network, safe from malicious and harmful traffic.

At certain Managed Service Levels, the customer will also be assigned a personal technician assigned to them to be available 24/7 to assist with issues, track problems and provide feedback from the time an issue is reported until it is resolved. It is this technician's responsibility to help mitigate confusion and provide a better channel for the flow of information – with the goal of providing a satisfied customer.

Application Specific Hardening

The Planet's Security Engineering Team, administrators and developers are experienced in securing a multitude of applications, services and tools and on many operating systems. This well-qualified staff is available to perform customized applications hardening services which are tailored to our customers needs. This additional assistance is available to all clients of The Planet for an additional fee.

Security Services at a Glance

Layer 1 – Attack Prevention Services

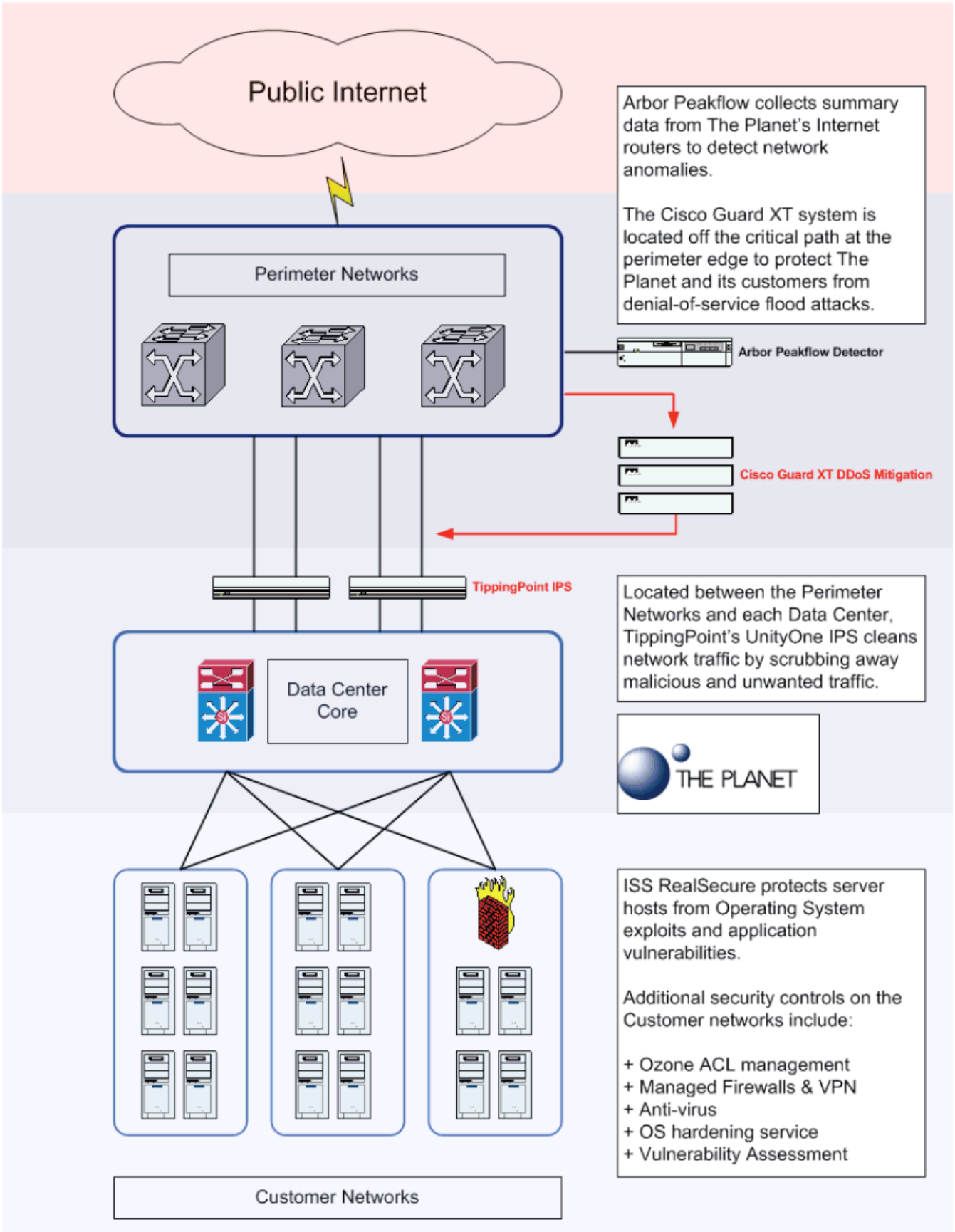
- **Ozone** Access Control List Management
- Virtual Private Network Tunnels
- Vulnerability Assessments
- Penetration Testing
- Operating System Hardening
- Custom Cryptographic Services

Layer 2 – Detection and Incident Response Services

- **Arbor** Peakflow DDoS Detection
- Firewall Protection
- **TippingPoint**'s **Unity One 2400** in-line network intrusion detection and prevention system
- **Cisco Guard DDoS Mitigation** deployed at the network edge in the event of an event detected by Arbor
- **ISS RealSecure** Host Based Intrusion Detection System
- Server Event Monitoring Services
- Server "Delta" Hardening
- System Integrity Checking

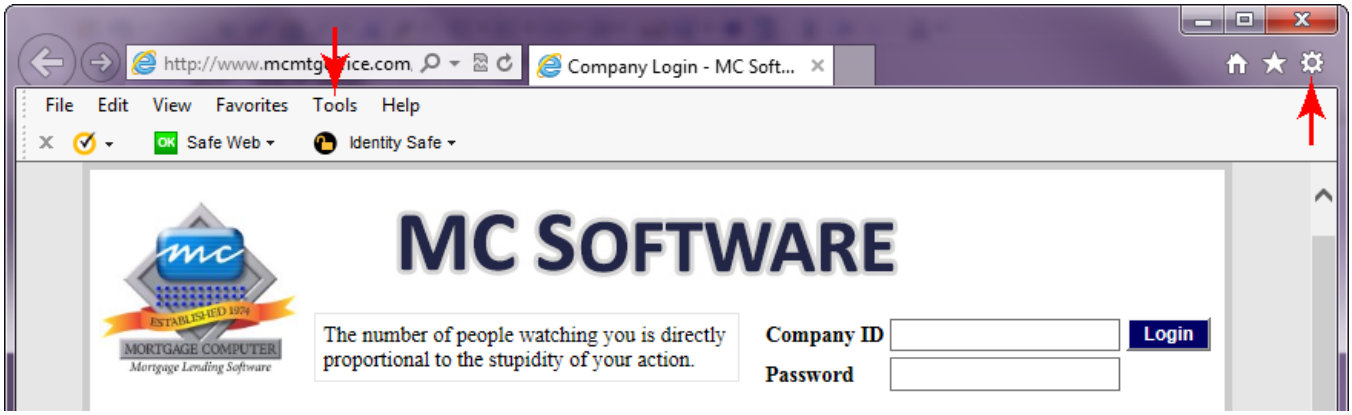
Layer 3 – Threat Elimination Services

- Managed Operating System Update Services
- Server Administrative Services
- Incident Response by Certified Security Engineers
- Application Specific Hardening

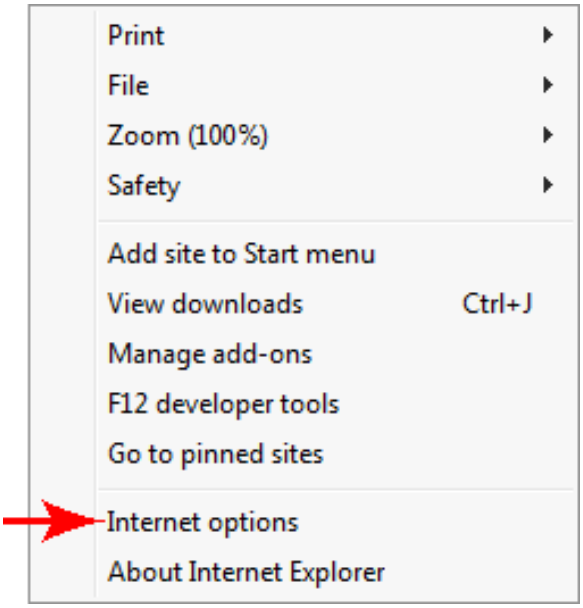

Public Internet
Perimeter Networks
Arbor Peakflow collects summary data from The Planet's Internet routers to detect network anomalies.
The Cisco Guard XT system is located off the critical path at the perimeter edge to protect The Planet and its customers from denial-of-service flood attacks.
Arbor Peakflow Detector
Cisco Guard XT DDoS Mitigation
TippingPoint IPS
Located between the Perimeter Networks and each Data Center, TippingPoint's UnityOne IPS cleans network traffic by scrubbing away malicious and unwanted traffic.
Data Center Core
THE PLANET
ISS RealSecure protects server hosts from Operating System exploits and application vulnerabilities.
Additional security controls on the Customer networks include:
+ Ozone ACL management
+ Managed Firewalls & VPN
+ Anti-virus
+ OS hardening service
+ Vulnerability Assessment
Customer Networks

Required Internet Explorer Browser Settings for MC Software

Open your browser and click on **Tools** in either of the two locations indicated below.

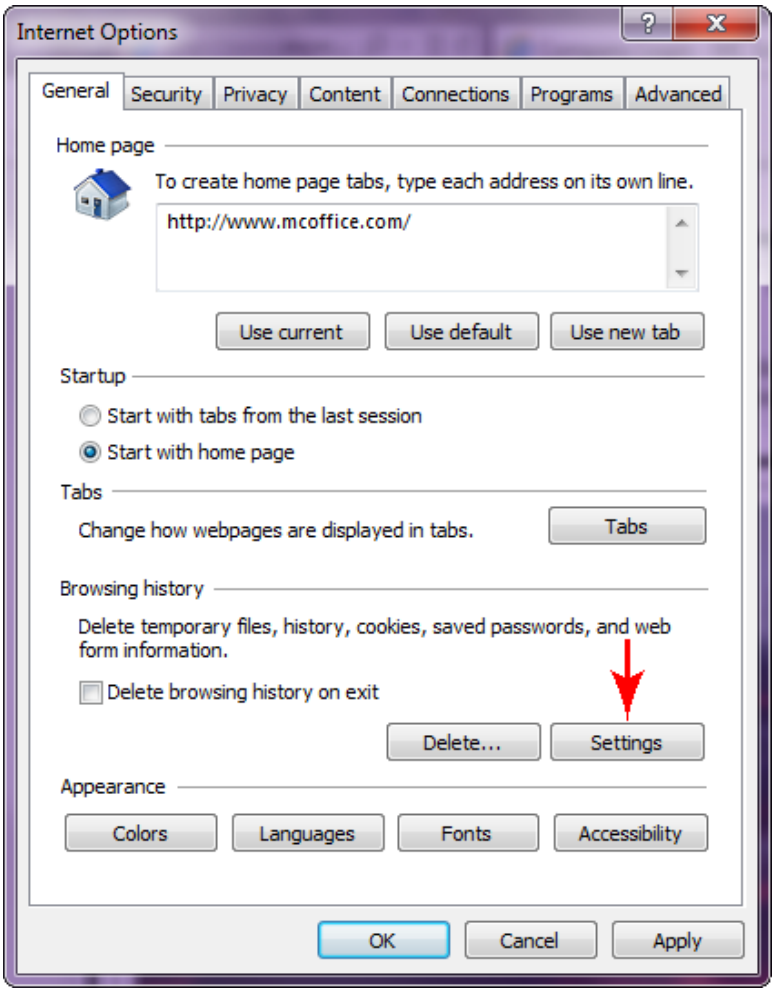


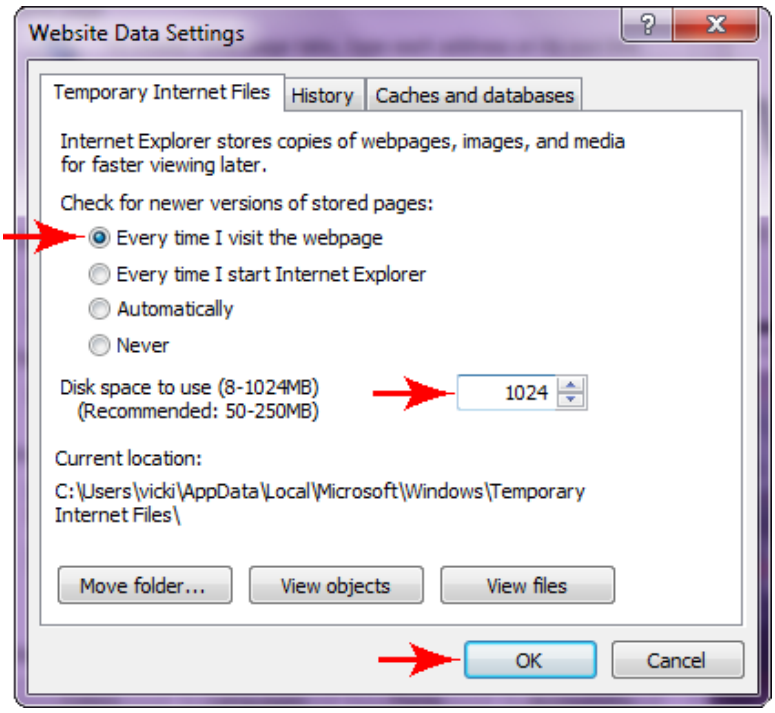
Select **Internet Options**.



Browsing History

Click **Settings** under **Browsing history**.

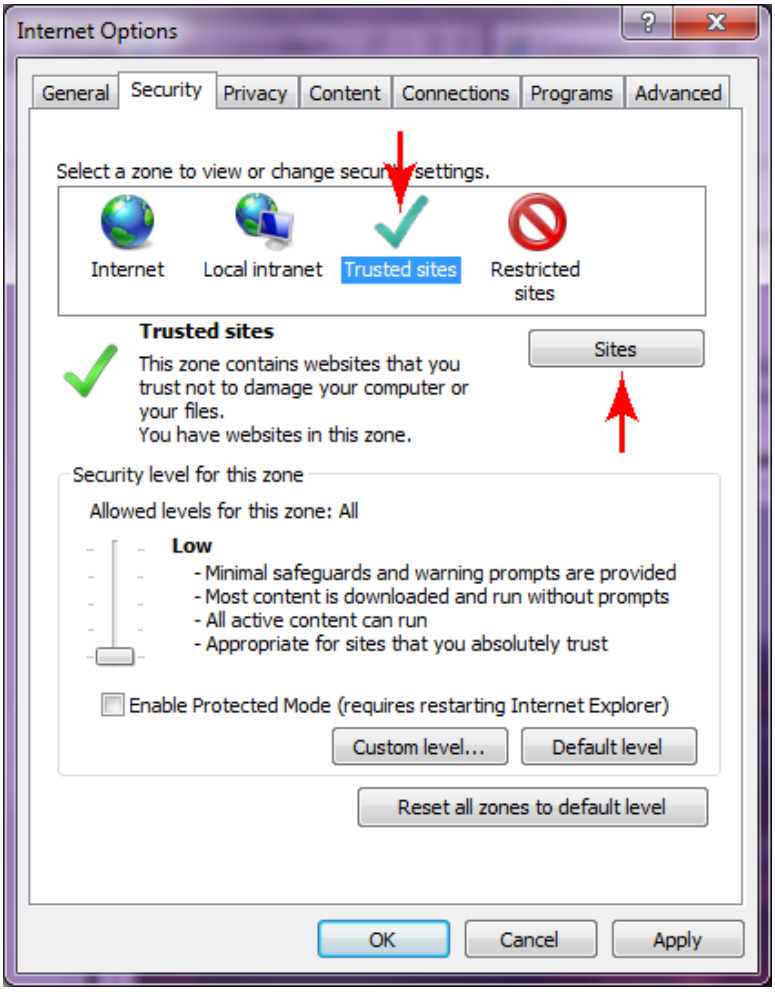




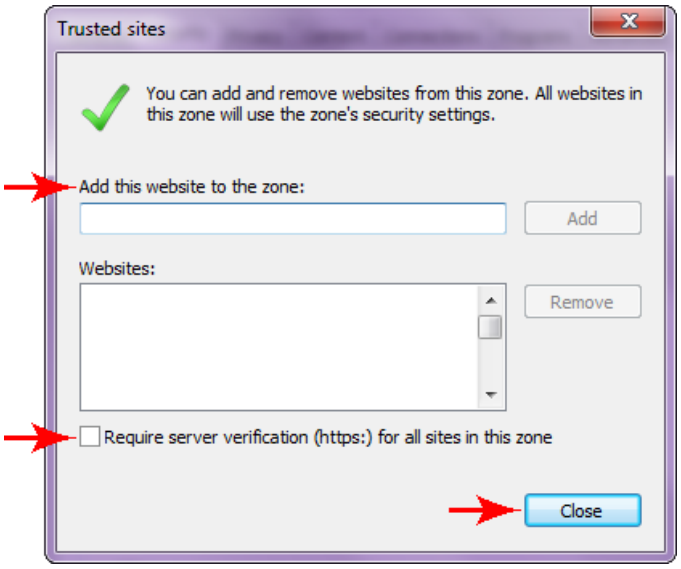
- Under **Check for newer versions of stored pages**, indicate **Every time I visit the webpage**.
- MC also recommends setting the **Disk space to use** to 1024.
- Click **OK**.

Security

On the **Internet Options** screen, select the **Security** tab.



Click on **Trusted Sites** and then click **Sites**.


Trusted sites
You can add and remove websites from this zone. All websites in this zone will use the zone's security settings.
Add this website to the zone:
Add
Websites:
Remove
Require server verification (https:) for all sites in this zone
Close

- Remove the checkmark from **Required server verification**.

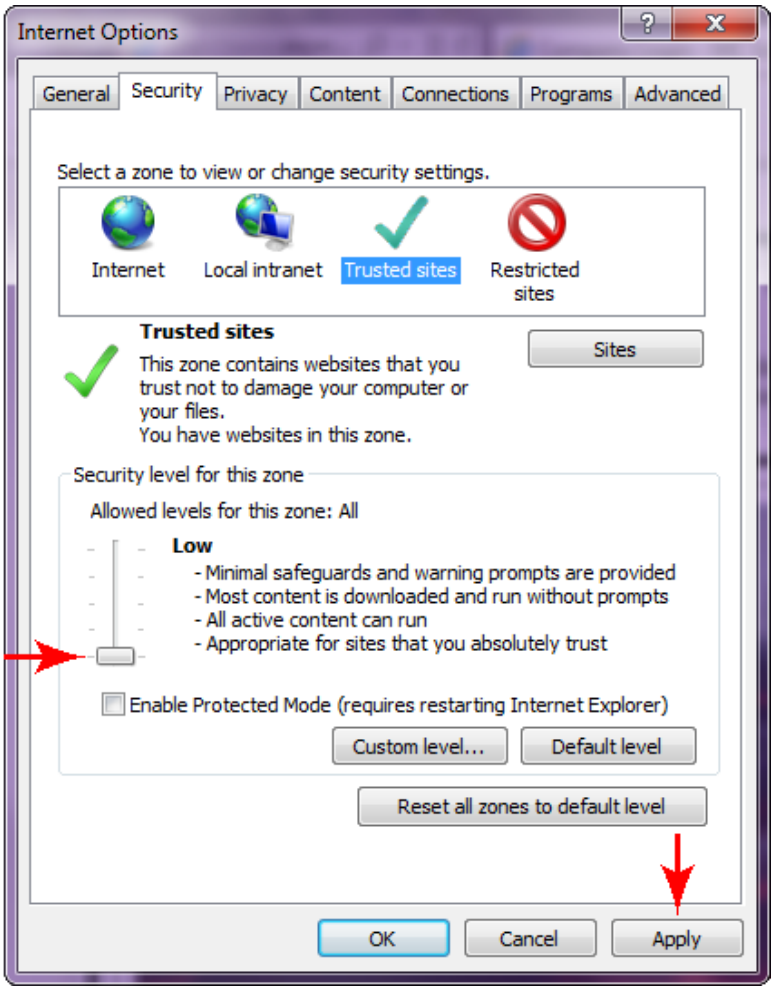
- Use the **Add this website to the zone** option to add individual Web sites. Enter the Web address and then click **Add**. The **Add** button will be activated when an address is typed in the field.

- Please add the following Web addresses:
  - mcmtgoffice.com
  - tmcmtgoffice.com
  - t1mcmtgoffice.com
  - t2mcmtgoffice.com
  - t3mcmtgoffice.com
  - t4mcmtgoffice.com
  - t5mcmtgoffice.com
  - t6mcmtgoffice.com
  - t7mcmtgoffice.com
  - t8mcmtgoffice.com
  - t9mcmtgoffice.com

- Click **Close**.

Security Level

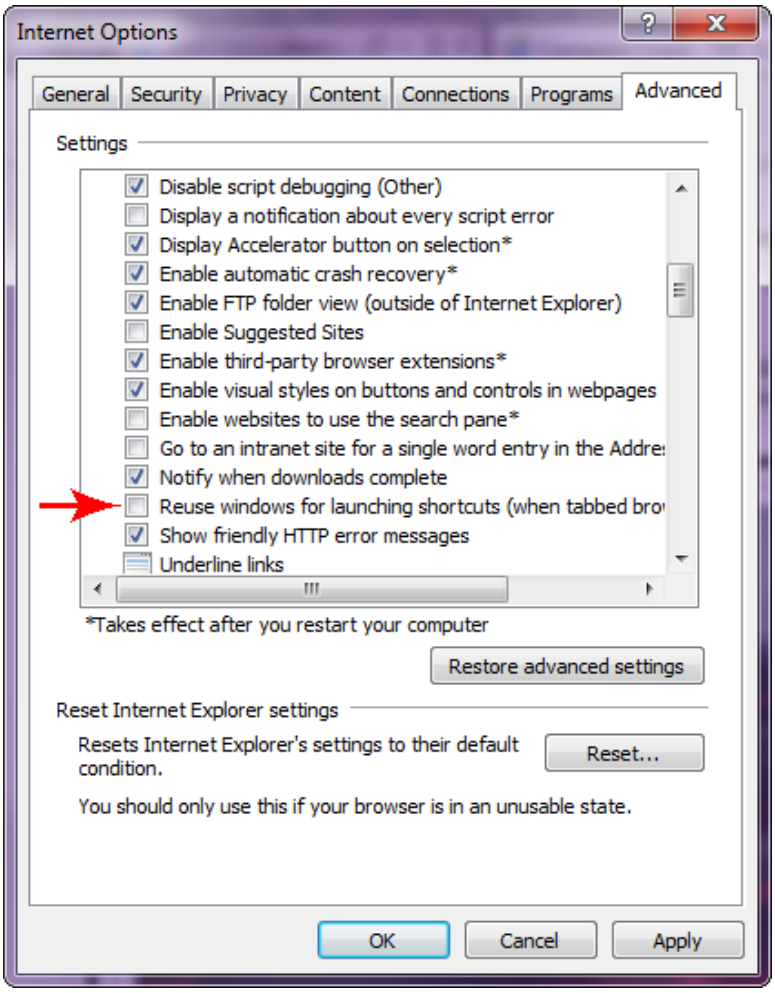
On the same **Security** screen, make sure the **Security level for this zone** is set to **Low**.



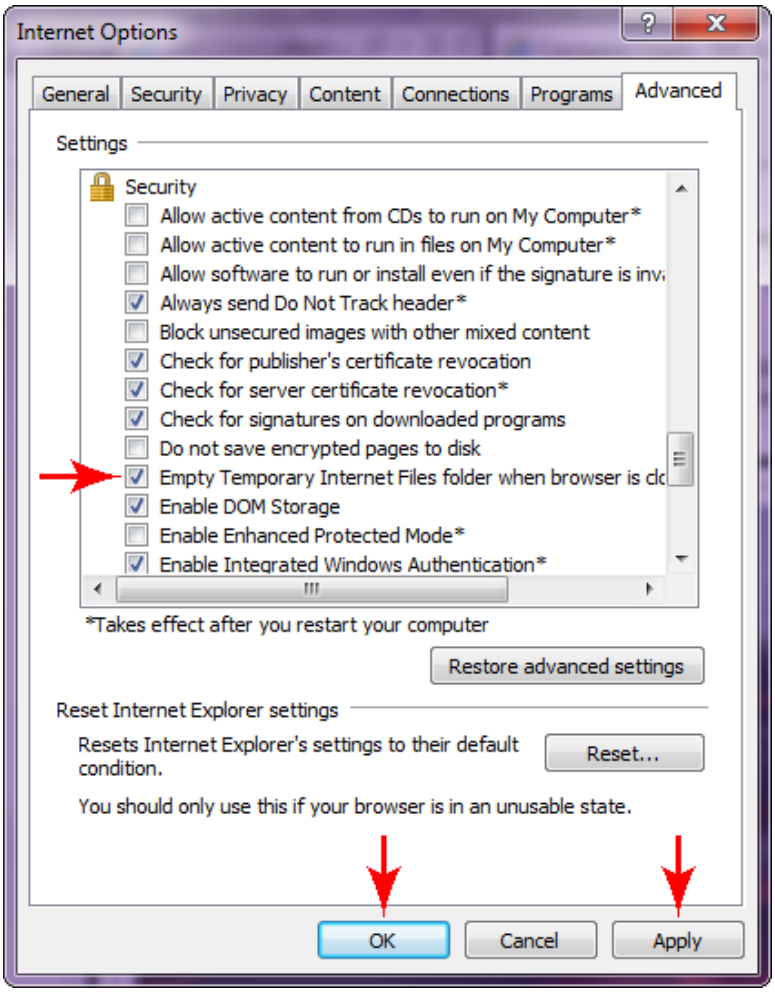
Click **Apply**.

Advanced

On the **Internet Options** screen, select the **Advanced** tab.


Internet Options
General
Security
Privacy
Content
Connections
Programs
Advanced
Settings
Disable script debugging (Other)
Display a notification about every script error
Display Accelerator button on selection*
Enable automatic crash recovery*
Enable FTP folder view (outside of Internet Explorer)
Enable Suggested Sites
Enable third-party browser extensions*
Enable visual styles on buttons and controls in webpages
Enable websites to use the search pane*
Go to an intranet site for a single word entry in the Addre
Notify when downloads complete
Reuse windows for launching shortcuts (when tabbed bro
Show friendly HTTP error messages
Underline links
*Takes effect after you restart your computer
Restore advanced settings
Reset Internet Explorer settings
Resets Internet Explorer's settings to their default condition.
Reset...
You should only use this if your browser is in an unusable state.
OK
Cancel
Apply

Scroll down in the settings and uncheck the box for **Reuse windows for launching shortcuts**.

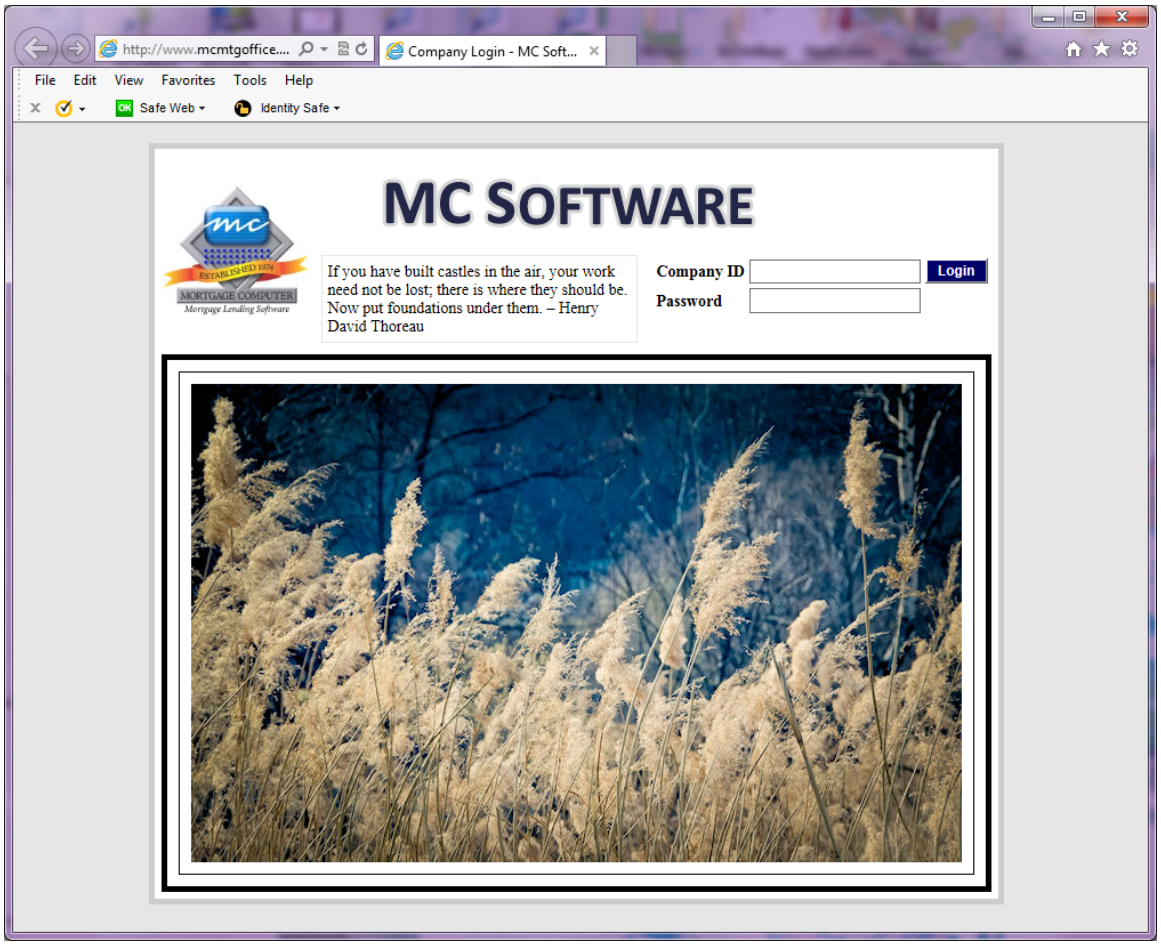

Internet Options
General
Security
Privacy
Content
Connections
Programs
Advanced
Settings
Security
Allow active content from CDs to run on My Computer*
Allow active content to run in files on My Computer*
Allow software to run or install even if the signature is inv
Always send Do Not Track header*
Block unsecured images with other mixed content
Check for publisher's certificate revocation
Check for server certificate revocation*
Check for signatures on downloaded programs
Do not save encrypted pages to disk
Empty Temporary Internet Files folder when browser is cl
Enable DOM Storage
Enable Enhanced Protected Mode*
Enable Integrated Windows Authentication*
*Takes effect after you restart your computer
Restore advanced settings
Reset Internet Explorer settings
Resets Internet Explorer's settings to their default condition.
Reset...
You should only use this if your browser is in an unusable state.
OK
Cancel
Apply

- Continue scrolling down and check the box for **Empty Temporary Internet Files folder when browser is closed**.
- Click **Apply** to save the changes and then click **OK**.

MC

Software

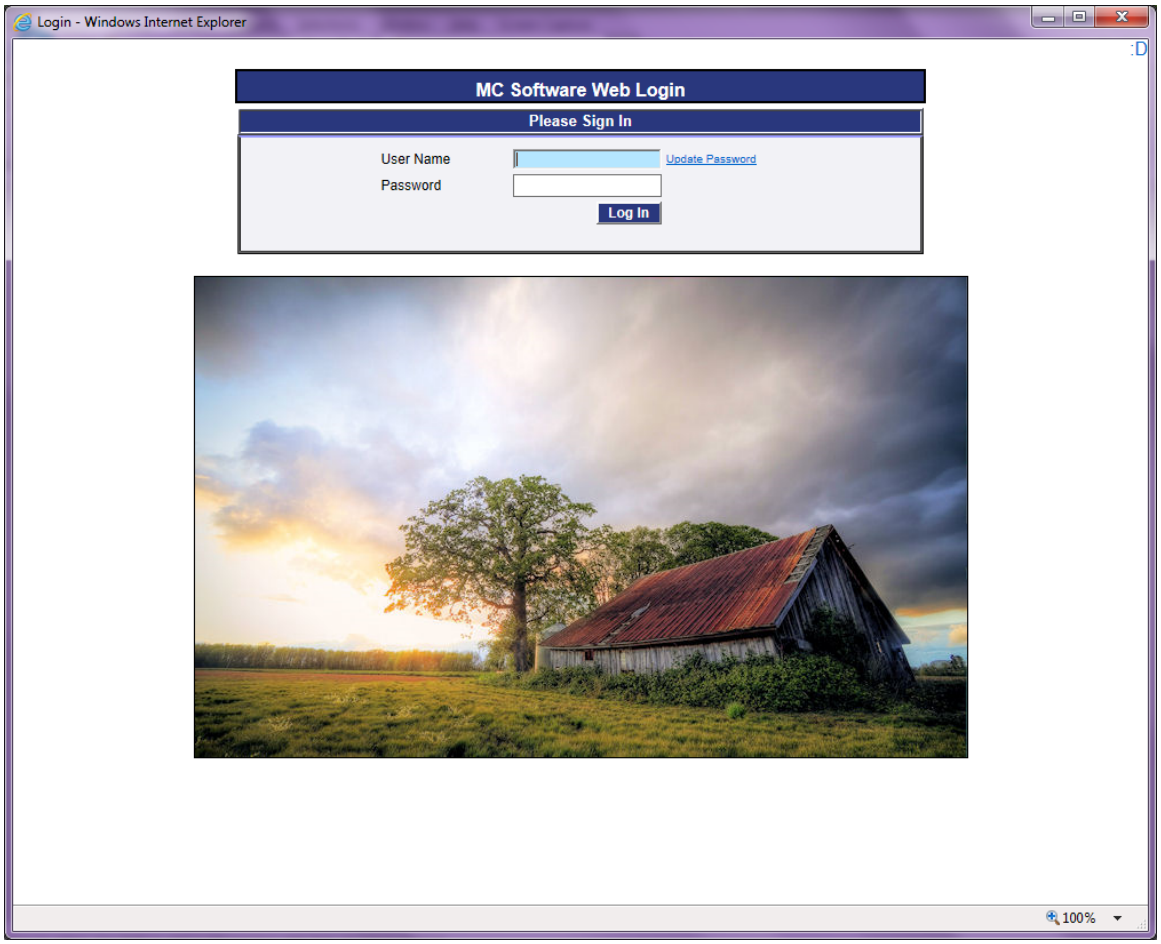
MC Software Company Login


http://www.mcmtgoffice....
Company Login - MC Soft...
File Edit View Favorites Tools Help
Safe Web
Identity Safe
MC SOFTWARE
MORTGAGE COMPUTER
Mortgage Lending Software
If you have built castles in the air, your work need not be lost; there is where they should be. Now put foundations under them. – Henry David Thoreau
Company ID
Password
Login

1. A different saying displays each time MC Software is selected.

2. Enter the Company ID and Password unique to your organization and click **Login**.

MC Software Web Login



User Name

Enter your assigned user name. The program will only allow one logon per user name and password, and requires the password to be **changed every 30 days**.

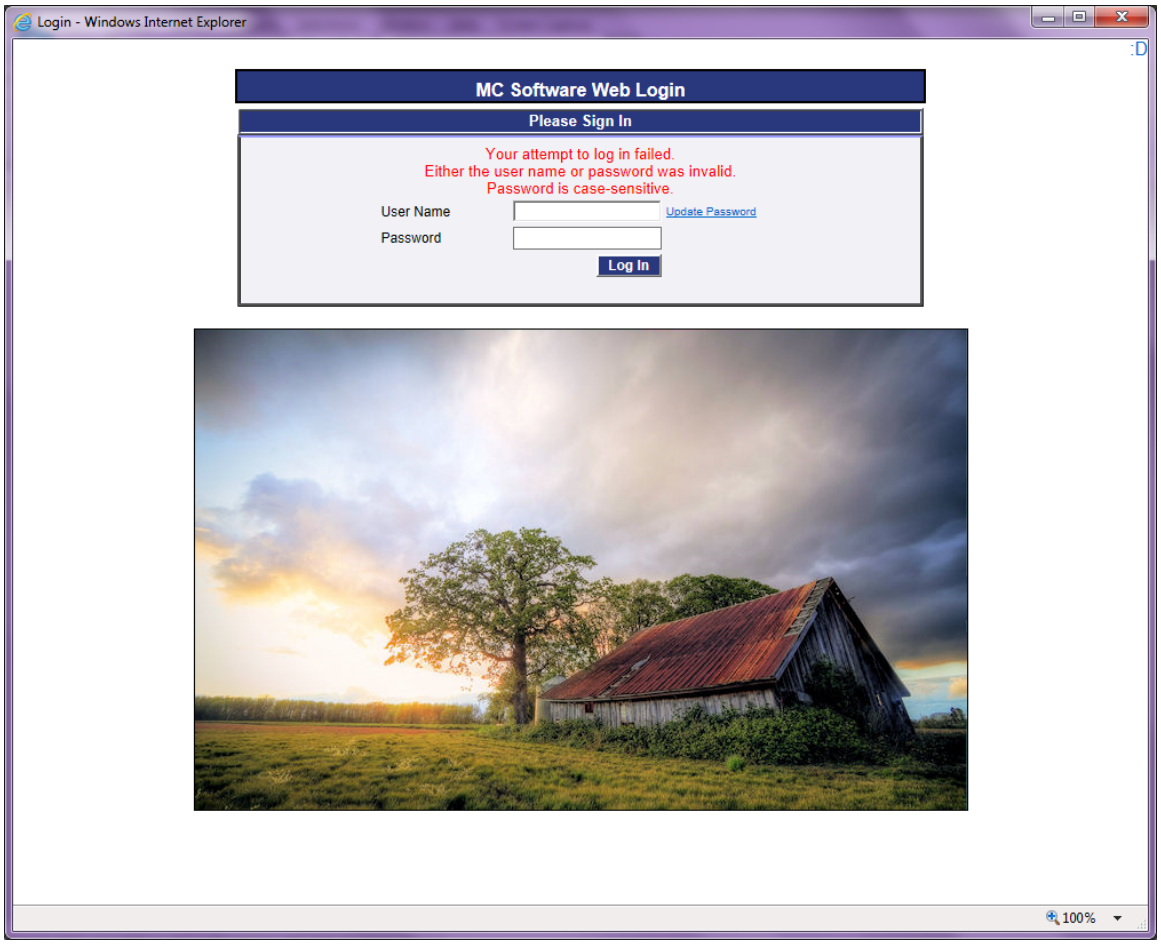
Password

Enter your corresponding password and click **Login**.

Update Password

An operator's password may be changed anytime. This option is used to update a password after entering your user name.

Update Password



Current Password

Enter your current password. The program requires the current password to be sure the correct operator is requesting the password change.

New Password

Enter your new password.

Confirm Password

Enter the new password again. The program asks for the new password twice and compares the two to make sure there were no typing errors. If they match, the new password is stored.

Update

Click **Update**. The program displays a message indicating the password has been updated.

MC Software Helpful Hints

Ampersand and Quotes

The ampersand (**&**) and quotes (**“ ”**) are used in programming language and are ***not to be used*** in the input of data.

Calendar Button

All date fields include the Calendar button. The program displays the current month and year. The current date is displayed in **red**. Within the calendar, select << to move backward *one year* and >> to move forward *one year*. Select < to move backward *one month* and > to move forward *one month*. Selecting the date from the calendar eliminates several keystrokes.

Check Box

More than one choice can be made. Press the space bar to make a check box selection. Click the check box once to unselect.

Date Fields

Dates fields can be entered as 041006; program displays 4-10-2006.

Display/Print

Click on the word **Display** to view and/or print a form while in the menu selection (1003 loan application, Good Faith Estimate, Underwriting Transmittal, etc.).

Drop-Down Menus

On drop-down menus where more than one choice can be made, hold the [Ctrl] key down and click the desired selections. To unselect, [Ctrl] click.

On drop-down menus, enter the first letter of the selection, then use the up and down arrow keys to locate the appropriate selection, e.g., state selection.

Exit/Close

If there is no **Back** or similar button on a screen, a different option from the main menu can be chosen to exit/close that selection.

Main MC Software Menu

On the main MC Software menu, bold black options marked with a open to display other options. The ones marked with a access the option.

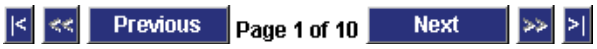
Phone Numbers

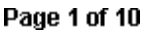
Phone numbers can be entered as 8016213900; program displays (801) 621-3900.

Enter an extension after the phone number, 80162139001234; program displays (801) 621-3900 Ext. 1234.

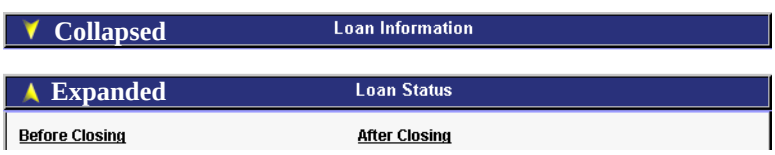
Print

To print the information displayed on the screen, right click and select the **Print . . .** option.

	The **Print** button within the MC Software displays reports, forms, etc., in PDF (portable document format). The toolbar within the PDF display screen contains options to save to a file, print, or e-mail. When printing reports and forms, do not use the browser **Print** button; use the Adobe **Print** button. Adobe Reader 7.0 or higher is required.
Radio Buttons	Only one choice can be made. Press the space bar to make a radio button selection. Double click the radio button to unselect.
Red Asterisk	A red asterisk (*) on any field indicates the field is mandatory.
Return	Click **Return** to go back to the previous screen.
Search Buttons	

	Indicates which page of the total number of pages is currently displayed.
	Advance to the next page.
	Advance forward or move backward 10 pages.
	Advance to the last page or move backward to the first page of the search.
	Move back to the previous page displayed.

Social Security Numbers	Social Security Numbers can be entered as 123456789; program displays 123-45-6789. The entire Social Security Number only displays in the 1003 loan application. Anywhere else, it displays as ***-**-6789.
Sort	Click on underlined column headers to sort listings numerically, alphabetically, etc. (whatever the column header indicates) as in Products Offered/Rate Sheet.
Tab Key	Use the Tab key to navigate through the fields. Shift Tab takes you back to the previous field.
Tax Identification Numbers (TIN)	Tax Identification Numbers, used when the borrower/seller is a corporation rather than an individual, can be entered as 123456789; program displays 12-3456789. The entire TIN only displays in the entry screen. Anywhere else, it displays as **-***6789.
Yellow Triangle	The yellow triangle in the top left corner of the header bar collapses (or expands) the box to display more information.



MC Software Security

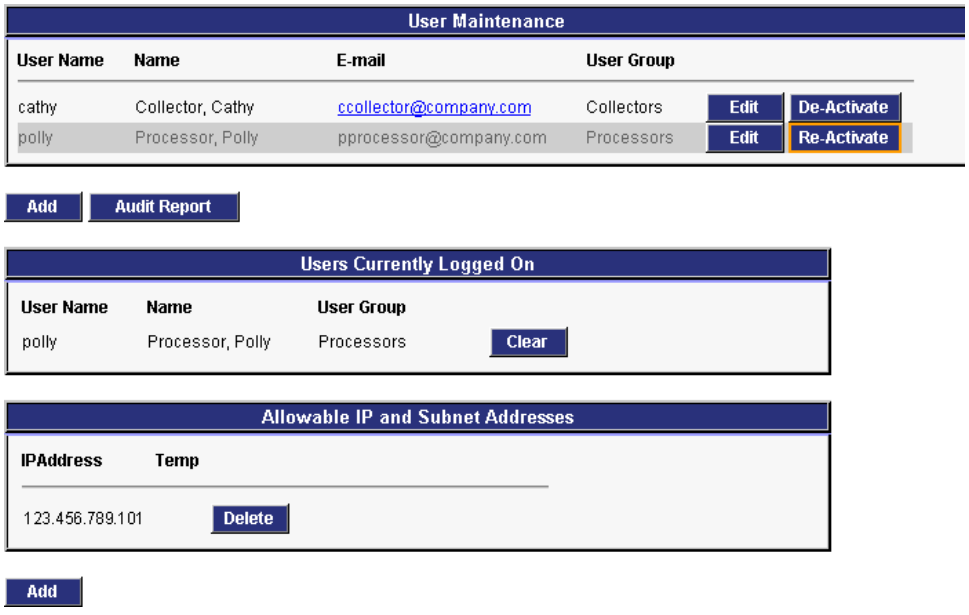
Login Names

The MC Software Maintenance program is flexible and powerful. **Login Names** and **User Groups** control who is allowed to access the program and what access privileges may be placed on any operator.

The administrator can assign operators to different user groups, permitting operators access to only those areas necessary to perform their duties. Each operator is identified by a unique user name and password. Each user name and password is maintained in Maintenance, along with the operator's access privileges to the functions of the MC Software programs.

Various *function* levels may be assigned to different operators, to limit access to certain areas within MC Software. Operators with a low security clearance may not be allowed access to higher, more sensitive areas. Thus, employees can be effectively *shut out* from sensitive parts of MC Software or programs assigned to others.

On the main MC Software menu, select **Maintenance > Company - Miscellaneous > Login Names**:



User Name

A 15-character field identifying the operator by name. Each operator of MC Software is identified via a unique user identification. The user name is the key for accessing the records for each operator. The program will only allow one logon per user name and password.

Name

First and last name of the operator.

E-mail

E-mail address of the operator. To send an e-mail, click on the e-mail address and the new e-mail message window displays.

User Group

Indicates the name if an operator is included in a user group.

Option to edit the user information.

Option to de-activate the user. Displays a message to verify the user is to be de-activated. If **OK** is selected, the user is "grayed out" and can no longer access MC Software. Toggles between **De-Activate** and **Re-Activate**. Clicking **Re-Activate** makes the user name functional again.

Prepares a report which indicates the menu items and Protected Fields to which operators have access. If the operator does not have access, the item will be grayed out and have a line striking through the item.

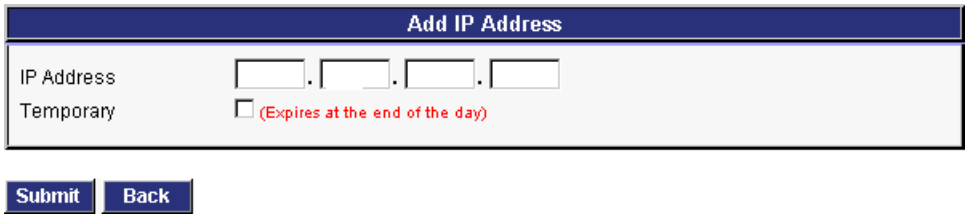
The program creates a .pdf (portable document format) of the report. The toolbar within the PDF report display screen contains options to **save** to a file, **print** or **e-mail** the report.

Users Currently Logged on

A listing of operators currently logged on to MC Software. If an operator is included in the listing but not actually using the program, this indicates they did not log out of the system. The **Clear** button will log the operator out of the program.

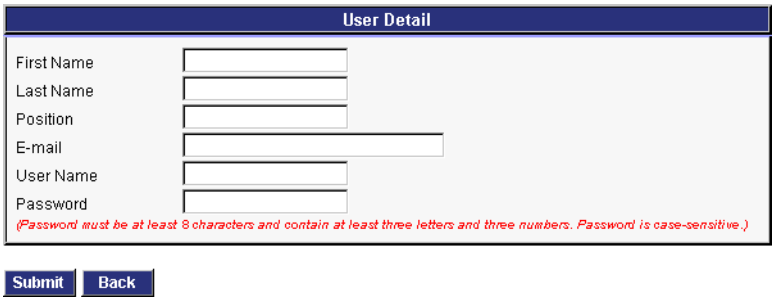
Allowable IP and Subnet Addresses

Each company hosted by Mortgage Computer will indicate an ACL (access control list), limiting the IP addresses by user name that are allowed to connect to the MC Software. With this option controlled by the administrator, you can allow some users to work remotely while limiting others to work from the office only. Click **Add** to create a new IP address.



Enter the IP address and click **Submit**.

Click on **Add** on the **User Maintenance** screen to create a new operator identification record. The following screen displays:



The password is a minimum of eight characters and must contain at least three letters and at least three numbers. Passwords expire every 30 days. The program will prompt the operator to enter a new password. The old password cannot be re-used as the new password. The user name and password are case sensitive. Enter the necessary information and click **Submit**.

User Security Access

To set up an individual operator's access within MC Software, click on **Edit** on the **User Maintenance** screen after creating a user name and password. The following screen displays:

Interviewer's License Number

Enter the operator's license number. The license number prints on Section X. Information for Government Monitoring Purposes of the 1003 loan application in the *Loan Originator Identifier* box.

Help On

When this option is enabled, the main MC Software menu will include a help button for each of the menu items. When the help button is clicked, documentation for that menu option displays. This option is extremely helpful when training new employees.

Vista

When the operating system is Windows Vista, this option must be enabled in order for the forms to print correctly. If this box is not checked, the Print Document options will not work properly.

Preferred Originator

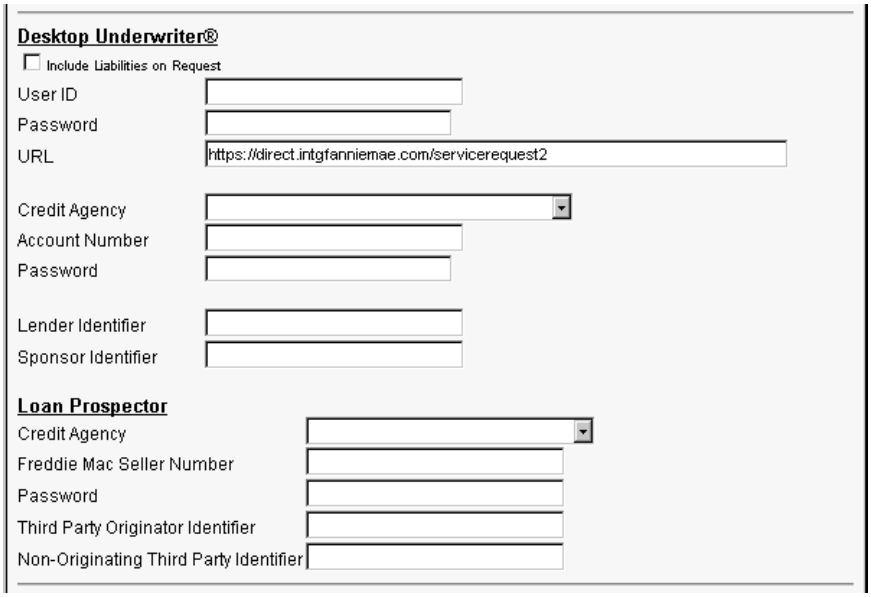
When this option is enabled, the operator's name will display in the list of Preferred Originators applicants can choose when submitting a loan application using the WebApp software. The preferred originator's Standard Field selections (Maintenance > Processing > Standard Fields) will default. However, if someone other than the preferred originator *accepts* the application, that loan originator's Standard Field selections will display. An e-mail will be sent to the Preferred Originator the applicant indicates notifying them a loan application has been submitted.

Send Foreclosure E-mail Reminder

If selected, an e-mail reminder will be sent to the e-mail address associated with the login name. The operator can indicate to have the e-mails sent a specified number of days prior to and after the Tracking Action Date. The verbiage for the message is set up in Maintenance > Servicing > Attorneys.

DU/LP Acct Override

If this option is enabled, the following screen displays to allow the input of the operator's user name and password to override the Desktop Underwriter and Loan Prospector information set up in **Company Information**.



User Group

After choosing a user group from the drop-down menu, click on **Apply Group Menu** to apply the group's parameters to a specific operator.

Help Group

As different languages become available, the operator will be able to select in which language the program displays.

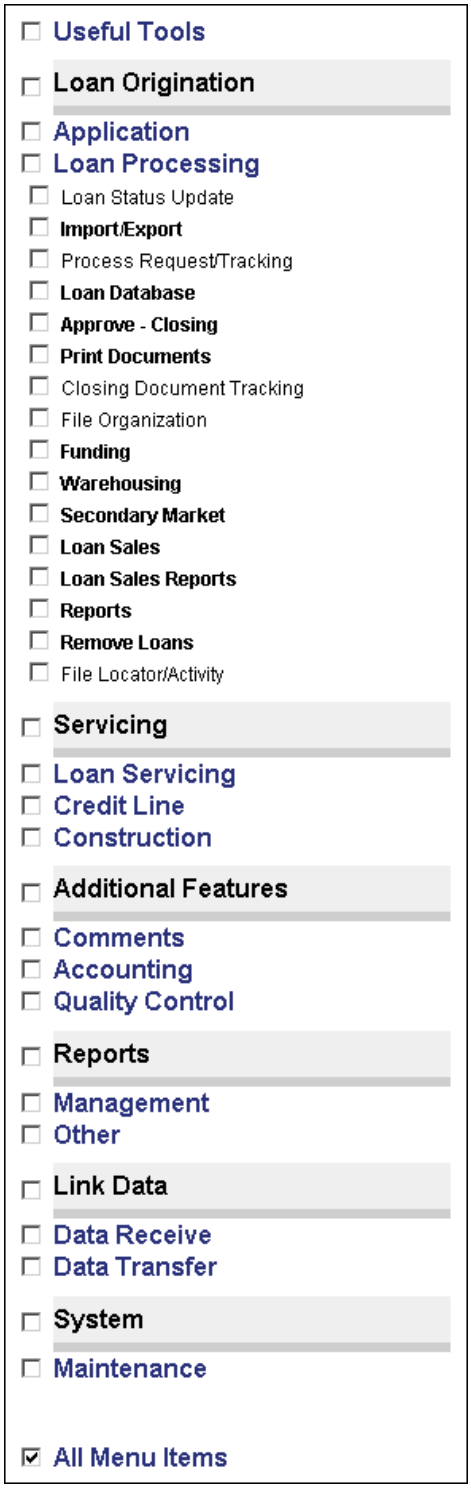
Reset User Password

Use this option to change an operator’s password. Enter the new password and click **Reset**.

Menu Items

Determine the items that will display on the main MC Software menu for each operator. If the item is not checked, it will not display and, therefore, the operator will not have access to that function. The operator's access within each of the main menu options can also be controlled. Click on the main menu option to display any additional program functions.

If **All Menu Items** is indicated, *all* menu items will display, including the additional program functions within the main menu options.



Protected Fields

Although all MC Software options may display on the main menu, an operator's access to the fields within those options can be protected. Click on **Protected Fields** and the following screen displays:

Comments

When Comments does not allow editing, the operator will be able to add, edit, and print the *Important Information*.

Employee Information

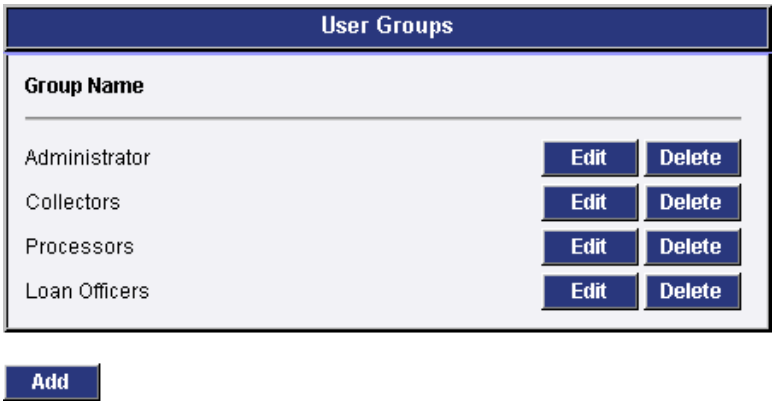
When Employee Information does not allow viewing, the operator will receive an accessed denied message when selecting a loan flagged as an *Employee* loan for either borrower, co-borrower, or additional borrower in the Master Record for all packages and the 1003 loan application in Processing.

Indicate the fields each operator will be able to modify/edit and click **Save**. If all fields will be accessible to the operator, click **Check All** and then **Save**.

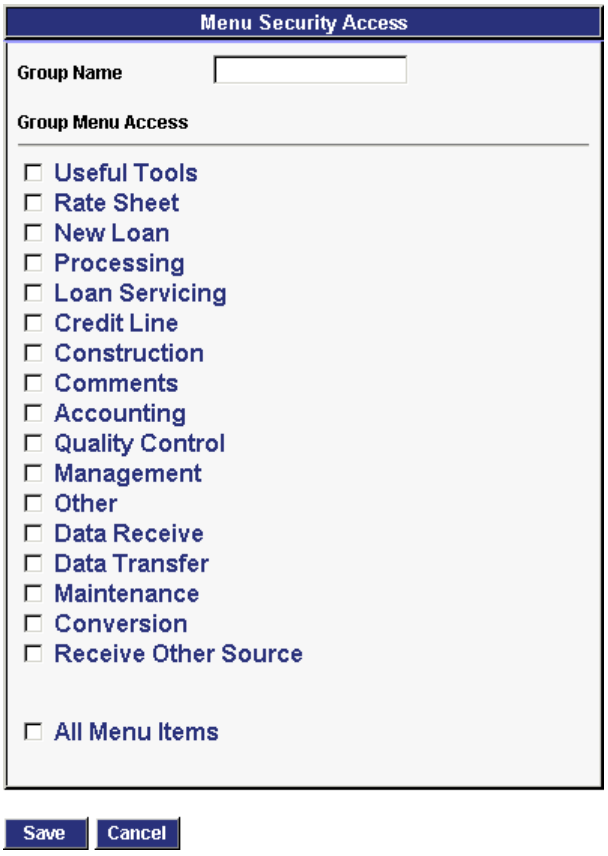
User Groups

User groups can be created for collectors, processors, loan officers, etc., to streamline the setup process and assure each operator's access within the user group is the same. The parameters set up here will be applied when the user group is selected in **Login Names**. Refer to **Login Names** for more information.

On the main MC Software menu, select **Maintenance > Company - Miscellaneous > User Groups**:



Click on **Add** to create a new user group or **Edit** to modify the menu functions each group will be able to access. The following screen displays:



Enter the Group Name and determine the menu options each group will have access to and click **Save**. If the item is not checked, it will not display and, therefore, the operator will not have access to that function. If **All Menu Items** is checked, *all* menu items will display.

*As with **Login Names**, the access within each of the main menu options can also be controlled. Click on the main menu option to display any additional program functions.*